Translator's Statement

I, Robert STOINSKI, Rennerle 10, 88131 Lindau (B), Germany, declare

1. that I am fully conversant with the English and German language,

2. that the attached copies are to my best knowledge and belief a true and correct translation in English language of the priority document of the German patent application No. 199 11 782.9 as filed with the German Patent and Trademark Office on March 17, 1999.

Date: May 08, 2008

(Robert Stoinski)

Enclosure:

Translation of Priority document,

Certificate:	1 page
Specification:	15 pages
Drawings:	2 pages

FEDERAL REPUBLIC OF GERMANY

Certificate

DeTeMobil Deutsche Telekom MobilNet GmbH in Bonn/Germany has filed a Patent Application with the title:

"Method for Using Standardized Bank Services via Mobile Radiotelephone Service"

with the German Patent- and Trademark Office on March 17, 1999.

The attached pieces are a correct and exact copy of the originally filed documents of this patent application.

The German Patent- and Trademark Office has preliminarily assigned to the application the symbols H 04 L and H 04 Q of the International Patent Classification.

Munich on 22. April 1999
German Patent- and Trademark Office
The President
by order
Faust

Filing Number: 199 11 782.9

Method for Using Standardized Bank Services via Mobile Radiotelephone Service

The invention relates to a method for using standardized bank services via mobile radiotelephone service.

For utilizing bank services, paperless and convenient ways for submissions, deposits and inquiries are increasingly requested. Due to the efficiency which can be achieved in this way, this development is being promoted on the part of banks, and for this purpose, German credit institutions have developed a method for general and comprehensive home banking by using, for example, a personal computer (PC) and a stationary network modem. This method, referred to as HBCI (Home Banking Computer Interface), rests on the cryptographic end-to-end encryption between a personal computer (client) on the customer side and the bank server (*cf.* Home Banking Computer Interface, Schnittstellenspezifikation, Version 2.0.1 of 2 February 1998). However, the low penetration in Germany of less than 10% of PC online access represents a first hindrance.

The mobile radiotelephone with approximately 15 million customers and high growth rates is spread considerably more widely. Here lies a potential key for mass market electronic access to bank transactions. Added to this is for the customer the capability of also gain mobile access to banking business.

The HBCI standard is intended as a platform for home banking in the German world of banking. It also appears obvious to build on this standard within the context of mobile radiotelephone-supported banking. Unfortunately, the HBCI protocol conceived for the Internet is too extensive for the direct projection onto the current GSM mobile telephone world. This involves the bandwidth necessary for the data transmission as well as also the requisite storage capacity and computing power on the side of the mobile telephone subscriber or his mobile station.

It is the task of the invention to propose a method which permits utilizing standardized bank services via mobile radiotelephone, wherein conventional mobile stations can be applied as a customer-end HBCI platform without additional devices.

This task is solved through the characteristics specified in claim 1.

The fundamental concept of this invention is the distribution of the customer-end HBCI system onto two components, the SIM card (subscriber identity module) used in the mobile station and an HBCI gateway.

For this purpose, two transmission routes are formed, firstly, between SIM card and HBCI gateway and secondly between HBCI gateway and bank server. On both subroutes cryptographic security is realized.

The HBCI gateway is thus inserted into the transmission path. It unpacks the HBCI protocol and converts the protocol sequence such that compatibility with the GSM SIM card and the GSM network standard is obtained. The HBCI gateway, lastly, exchanges the converted protocol with an SIM card used at the customer end. Accordingly, transformation between HBCI, used at the bank end, and the transmission protocol, used at the mobile radiotelephone end, takes place. The task of the HBCI gateway is essentially the reduction of the data to be transmitted to a GSM compatible size.

As a carrier service for the information exchange between HBCI gateway and mobile telephone subscriber can serve, for example, the Short Message Service or GPRS.

From the viewpoint of the bank server an HBCI protocol conforming to standard is entirely used, wherein between bank server and HBCI gateway the security protocol defined by the HBCI is applied. Between HBCI gateway and SIM card another security protocol is employed. This corresponds to a protocol which, in terms of data quantity, is reduced but which in terms of security technology is equivalent to HBCI.

Instead of the PC, conventionally used in online banking, the SIM chip card now assumes the functions of the customer system as far as the user dialog as well as also the security functions are concerned. This is made possible through a new standardized technology with the name SAT (SIM Application Toolkit), which permits the mobile radiotelephone chip card (SIM card) to take on the role of the service control.

The SIM card, as well as also the bank computer, communicate with each directly with the HBCI gateway exclusively; thus, it assumes a proxy function, i.e. a representative function of the particular partner.

Said transformation also entails a transformation of the security mechanisms applied; while between the gateway and the bank world the HBCI protocol is used, at the GSM side a separate security protocol is applied.

A preferred further development of the invention provides that a method is applied which permits, after the SIM card personalization, generating and storing securely in the SIM card cryptographic keys. To this end by the HBCI gateway or the bank a special PIN letter is generated. The input of the PIN on the mobile telephone generates in the SIM card the key specific to the customer.

In this way, a secure, encrypted communication route between HBCI gateway and SIM card is set up without endangerment by "man-in-the-middle" attacks, for example through the network operator.

In the following the invention will be explained in conjunction with an embodiment example with reference to several Figures in the drawing. Based on the drawings and their description, further characteristics and advantages of the invention are evident.

Figure 1	shows schematically the devices required according to the invention for the bank services via mobile radiotelephone service.
Figure 2	shows by example a flowchart for the initial enabling of the bank services via online subscription.

The following embodiment example is based on the RDH variant for HBCI and on a symmetric triple DES solution (DES = Data Encryption Standard) at the GSM end.

In Figure 1 are schematically depicted the devices involved in the described method. Shown is a mobile station 1, comprising an end device 2 and a subscriber identity module 3 (SIM), by means of which a mobile radiotelephone subscriber can communicate via the air interface 5 with the mobile radiotelephone network, represented as base station 6.

To utilize the services, the mobile telephone subscriber must establish a connection with his bank 9 via the mobile radiotelephone network. The bank services are transacted via a special bank server 10, which utilizes a protocol, defined according to the HBCI standard, for the electronic communication with the subscriber.

At the GSM air interface 5 the GSM standard encryption 12 is applied. Above it lies on the application level a triple DES encryption 11, which secures the route between SIM card 3 and HBCI gateway 7. The route between HBCI gateway 7 and bank 9, or bank server 10, respectively, is subject to the standard HBCI protocol in the RDH variant, wherein an asymmetric RSA encryption method 13 is employed.

Since the HBCI gateway 7 assumes functions relevant to security, the possibility exists that it is being operated directly in the bank computer centers. Setting up the HBCI gateway at the particular network operator is also possible.

To secure the route between HBCI gateway 7 and SIM card 3, it is necessary to define a secret key Ksms between the gateway 7 and the SIM card 3. In order to ensure absolutely the secrecy of the key Ksms, a method is proposed in which the bank mails to the mobile radiotelephone subscriber in a PIN letter an initialization PIN which the subscriber enters once into the mobile telephone 2. In the SIM 3 as well as in the HBCI gateway 7, therefrom the key Ksms is derived by means of a suitable algorithm. This ensures that third parties do not have knowledge of this key. The security method will be explained in detail later.

To the subscriber can be offered, for example, business events such as account status inquiry, recent transactions and transfer orders. In every case encryption of the messages with Ksms takes place.

Actions are customarily initiated by the user via the operator control of the mobile radiotelephone 2.

For this purpose, it is possible for the SIM card 3 to set a separate menu item, for example "mobile banking", on the end device. If the set-up menu item is selected, the subitems "account status", "transactions", "transfer" and "configuration" can, for example, be offered.

Based on the fact that the limited capabilities of a mobile telephone keypad demand an optimized user guidance, it is possible to provide as an option that in particular the personal bank connection is stored in the SIM card 3 such that it only needs to be entered once.

In order to ensure that unauthorized persons are not in a position to initiate bank transactions, a local PIN should be queried with each transaction request. This PIN is locally administered by the card.

In the following an example of the sequence of the subscription of the subscriber is specified.

- Enabling the banking service takes place according to the representation in Figure 2 by selecting a set-up menu item "configuration" (see above); hereupon in a next step the bank routing number and account numbers of the personal account are queried as well as initialization PIN and local PIN for the bank user. The data of the personal bank connections are stored in the card. In a further step, from the initialization PIN and an initialization key KIV, derived from a master key, the card calculates a key Ksms to secure the communication between HBCI GSM gateway and SIM card. The query of the local (card) PIN serves as a protection against unauthorized subscription attempts.
- After calculating Ksms, the SIM card reports to the HBCI gateway the

subscription request. Hereupon the local key generation takes place at the HBCI gateway as well as the first dialog with the HBCI bank system. The HBCI gateway further sends a message to the card which accomplishes the adaptation of the bank menu title and the complete activation of the application.

Security

A highly important characteristic of the described method is its security. The goal of the security concept is primarily the prevention of misuse (Authentication of the customer). It is furthermore important to ensure the confidentiality of the transmitted data (encryption of the transmission). Both requirements are realized by means of cryptographic methods.

Security Sections

The entire route from mobile telephone 1 of the customer up to the HBCI server 10 of the bank is structured into two security sections. The first section extends from the SAT SIM card 3 to the HBCI gateway 7. The route from the HBCI gateway 7 to the bank server 10 forms the second security section.

Security Section 1: SAT SIM to HBCI gateway

The security functions of this section are essentially determined by assigning and using a special key Ksms. With this 128 bit triple DES key 11 all messages exchanged between SAT SIM 3 and HBCI gateway 7 are encrypted and signed.

The Ksms secures the connection from the SIM 3 to the HBCI gateway 7. The Ksms authenticates the subscriber as well as also the HBCI gateway and is also used for the encryption of this route. The Ksms is a specific key of the bank application and remains hidden to the network operator. In order to ensure this, the following method is, for example, applied for the generation:

During the card personalization, the network operator applies onto all cards, together with the bank application, a KIV for generating the Ksms specific to each customer. The KIV is generated with the aid of a master key and a number individual to each SIM card. Before subscription to the service, the subscriber receives the data of his bank including a 20-digit PIN. During the initialization of the SAT application (online subscription) from the PIN, the customer key Ksms proper is generated with the aid of the KIV (encrypting of PIN, bank routing number and the account number through triple DES with KIV as the key).

To generate the Ksms in the HBCI gateway 7, the PIN must also be transferred to the gateway operator. Optionally the generation of the PIN at the HBCI gateway and transfer to the bank is possible.

Authentication between subscriber and HBCI gateway takes place through the knowledge via the PIN exchanged in writing. Between network operator and HBCI gateway operation, additionally, a master key for generating the KIVs must be exchanged. This master key authenticates therewith additionally the HBCI gateway. Moreover, optionally an additional authentication of the customer can take place via the knowledge of his mobile connection:

At the HBCI gateway, evaluation of the calling line identification (CLI) of the transmitted SAT SIM can be carried out. For this purpose the mobile radiotelephone number of the customer must be administered in the HBCI gateway.

Security Section 2: HBCI gateway to the system of the credit institution

On the interface from HBCI gateway 7 to the bank 9 an unmodified HBCI protocol is applied. In the implementation represented here, the RDH variant is used. In the model of the HBCI specification, the HBCI gateway represents the customer system. On the HBCI gateway the public and the private signing and encryption keys for each customer are stored.

The mechanism of the authentication of the public customer as well as bank keys must take place be based on contractual provisions between the operator of the HBCI gateway 7 and the operator of the bank server 10. Should there be no implicit mutual trust between these parties, PIN letters or also certificates can be employed.

The following table provides an overview over the keys used in the method

Key	Application	Generation	Repository	Known by
Ki	GSM authentication air interface	network operator during card personalization	SIM, authentication center network operator	network operator
Kc	GSM encryption air interface	network + SIM during setup of connection	mobile telephone + GSM network	network operator
CKpub	HBCI public key (encryption) of customer	HBCI gateway with subscription	HBCI gateway, bank	gateway operator, bank
CKpriv	HBCI private key (encryption) of customer	HBCI gateway with subscription	HBCI gateway	gateway operator
AKpub	HBCI public key (authentication) of customer	HBCI gateway with subscription	HBCI gateway, bank	gateway operator
AKpriv	HBCI private key (authentication) of customer	HBCI gateway with subscription	HBCI gateway	gateway operator
CBpub	HBCI public key (encryption) of bank		bank, HBCI gateway	gateway operator, bank
CBpriv	HBCI private key (encryption) of bank		bank	bank
ABpub	HBCI public key (authentication) of bank		bank, HBCI gateway	gateway operator, bank
ABpriv	HBCI private key (authentication) of bank		bank	bank
KIV	initialization key	network operator	SIM card	SIM card, HBCI gateway
Ksms	encryption and authentication SAT SIM to gateway	HBCI gateway before subscription as well as SAT SIM with subscription	HBCI gateway, SAT SIM	gateway operator, indirectly also customer

The proposed method offers a high level of security. The technical components involved (SIM, mobile radiotelephone, HBCI gateway) are far less susceptible to misuse than, for example, a personal computer. From the point of view of the subscriber with the present technical concept a novel service is provided concomitant with a high security standard.

Patent Claims

1. Method for using standardized bank services via mobile radiotelephone, wherein the data transmission between a bank server and a mobile station builds on the HBCI transmission method,
characterized in
that an HBCI gateway is inserted into the transmission path between the bank server and the mobile station, which carries out a transformation between the HBCI transmission method used at the bank end and a transmission method used at the mobile radiotelephone end.

2. Method as claimed in claim 1, characterized in that a splitting of the customer-end HBCI system into two components, the SIM card of the mobile station and the HBCI gateway takes place.

3. Method as claimed in claim 1 or 2, characterized in that two transmission routes are formed, firstly between SIM card and HBCI gateway and secondly between HBCI gateway and bank server.

4. Method as claimed in one of claims 1 to 3, characterized in that the HBCI protocol is unpacked by the HBCI gateway and its protocol sequence is converted such that compatibility with the GSM SIM card and the GSM network is obtained in order for an exchange of the converted protocol with the SIM card is to be possible.

5. Method as claimed in one of claims 1 to 4, [characterized in] that as a carrier service for the information exchange between HBCI gateway and mobile station serves a GSM data transmission service, in particular the Short Message Service, GPRS or USSD.

6. Method as claimed in one of claims 1 to 5, [characterized in] that on both subroutes a cryptographic security is realized.

7. Method as claimed in one of claims 1 to 6, characterized in that between bank server and HBCI gateway the security protocol defined by HBCI is applied and between HBCI gateway and SIM card a second security protocol is employed.

8. Method as claimed in one of claims 1 to 7, characterized in that the second security protocol corresponds to a protocol reduced in terms of data quantity but equivalent to HBCI in terms of security technology.

9. Method as claimed in one of claims 1 to 8, characterized in that a cryptographic key (Ksms) specific to each subscriber is securely generated and stored in the SIM card for use in the second security protocol after the regular SIM card personalization.

10. Method as claimed in one of claims 1 to 9, characterized in that the generation of the key (Ksms) specific to the subscriber is generated in the SIM card by entering an initialization PIN on the mobile telephone.

11. Method as claimed in one of claims 1 to 10, characterized in that the subscriber is informed per PIN letter by the bank of the PIN for generating the key (Ksms).

12. Method as claimed in one of claims 1 to 11, characterized in that during the card personalization by the mobile radiotelephone network operator together with the bank application, an initialization key KIV, derived from a master key and a SIM card-individual number, for generating the Ksms specific to the subscriber is applied onto all SIM cards.

13. Method as claimed in one of claims 1 to 12, characterized in that before subscription to the service the subscriber receives the data of his bank including an initialization PIN.

14. Method as claimed in one of claims 1 to 13, characterized in that during the initialization of the application, i.e. during subscription, with the aid of the KIV, from the initialization PIN the key Ksms is generated through triple DES using the local PIN, the bank routing number and the account number.

15. Method as claimed in one of claims 1 to 14, characterized in that for the generation of the Ksms in the HBCI gateway the initialization PIN is transferred to the gateway operator.

16. Method as claimed in one of claims 1 to 14, characterized in that the generation of the initialization PIN takes place at the HBCI gateway and this is transferred to the bank.

17. Method as claimed in one of claims 1 to 16, characterized in that the authentication of the two involved sites, mobile radiotelephone subscriber and HBCI gateway, takes place by knowledge of the initialization PIN exchanged in writing.

18. Method as claimed in one of claims 1 to 17, characterized in that between mobile radiotelephone network operator and HBCI gateway operator a master key is exchanged.

19. Method as claimed in one of claims 1 to 18, characterized in that an additional authentication of the subscriber takes place via the identification of his mobile connection thereby that an evaluation of the calling line identification (CLI) is carried out.

Abstract

The invention relates to a method for using standardized bank services via mobile radiotelephone, wherein the data transmission between a bank server and a mobile station builds on the HBCI transmission method. The problem is that the HBCI protocol conceived for the Internet is too extensive for the direct projection onto the current GSM mobile telephone world. The invention is characterized in that an HBCI gateway is inserted into the transmission path between the bank server and the mobile station, which carries out a transformation between the HBCI transmission method used at the bank end and a transmission method used at the mobile radiotelephone end.

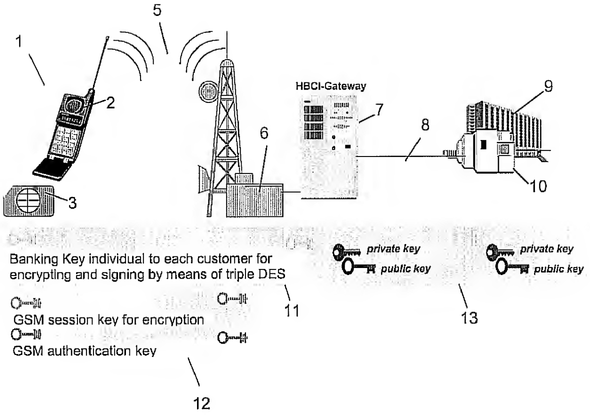
5
1
2
HBCI-Gateway
9
7
8
6
3
10
Banking Key individual to each customer for encrypting and signing by means of triple DES
private key
public key
private key
public key
11
13
GSM session key for encryption
GSM authentication key
12

FIG. 1

Online-Subscription

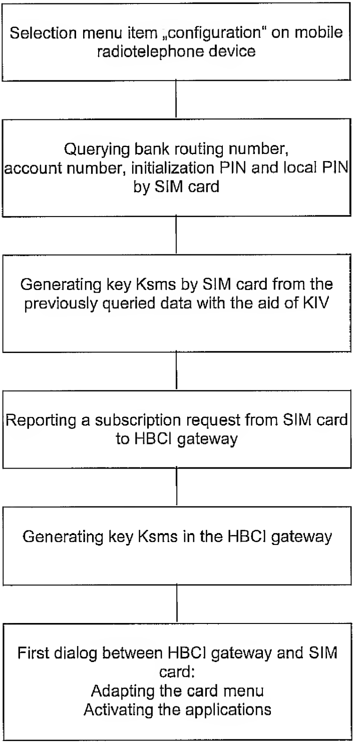
Selection menu item „configuration“ on mobile radiotelephone device
Querying bank routing number, account number, initialization PIN and local PIN by SIM card
Generating key Ksms by SIM card from the previously queried data with the aid of KIV
Reporting a subscription request from SIM card to HBCI gateway
Generating key Ksms in the HBCI gateway
First dialog between HBCI gateway and SIM card:
Adapting the card menu
Activating the applications

FIG. 2